Software Security: Shifting the Paradigm From Patch Management To Software Assurance

Dependency on information technology places software assurance as a key element of national security and homeland security. Vulnerable software is a risk to a broad spectrum of business and mission operations, including everything from process control systems to commercial application products that support and enable them. Software enables and controls the nation's critical infrastructure, and to ensure the integrity of that infrastructure, the software must be reliable and secure. However, informed consumers have growing concerns about software security, suppliers' capabilities to exercise a minimum level of responsible practice, and the scarcity of practitioners with requisite competencies to build secure software. Security-enhanced processes and technologies are required to build trust into software acquired and used by government and those who operate our nation's critical infrastructure.

The Department of Homeland Security (DHS) Software Assurance Program is grounded in the "National Strategy to Secure Cyberspace." DHS began the Software Assurance Program as a focal point to partner with the private sector, academia, and other government agencies to improve software development and acquisition processes. Through public-private partnerships, the Software Assurance Program framework shapes a comprehensive strategy that addresses people, process, technology, and acquisition throughout the software life cycle. Our efforts seek to shift the paradigm away from patch management and to achieve a broader ability to routinely develop and deploy trustworthy software products. These efforts will contribute to the production of higher quality, more secure software. The DHS Software Assurance Program is designed to lead the development of practical guidance, review tools, and promote research and development investment in cyber security. The overall goal is secure and reliable software supporting mission requirements, enabling more resilient operations.

Through hosting and co-hosting various forums and workshops, we will continue to leverage collaborative efforts of public-private working groups. DHS initiatives such as the "Build Security In" Web site and the "Software Assurance Common Body of Knowledge" will continue to evolve and provide practical guidance to software developers, architects, and educators on how to improve the quality, reliability, and security of software. These two initiatives are discussed this month in *Engineering Security Into the Software Development Life Cycle* (see page 4) and *Creating a Software Assurance Body of Knowledge* (see page 5).

DHS collaboration with standards organizations is focused on evolving standards to reflect guidance for appropriate levels of responsible practice for software security. To be relevant in today's global economy that relies on outsourcing of software and information technology services, models and standards that provide criteria to guide and appraise process improvement and support international commerce must explicitly address security (see *Sixteen Standards-Based Practices for Safety and Security* on page 11).

This DHS-sponsored issue of CrossTalk addresses the value of software security; I hope you will take the time to read, understand, and apply the principles and techniques discussed in this month's articles. I encourage you to discover more about our DHS Software Assurance Program and learn more about proven security practices by visiting us at <http://BuildSecurityIn.us-cert.gov> and join others in our expanding software assurance community of practice.

Joe Jarzombek

Joe Jarzombek, Project Management Professional (USAF Lt. Col., Retired)
Director for Software Assurance
National Cyber Security Division
Department of Homeland Security